http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (8): 1505-1513, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1505.1513

QUAD Based Secured Multipath Routing Protocol for Mobile Ad hoc Networks

[1]J. Viji Gripsy and [2]Anna Saro Vijendran
[1]Department of Computer Science, Psgrkc, Coimbatore, India
[2]Department of MCA, S.N.R. Sons College, Coimbatore, India

Abstract: Routing mechanism plays a vital role in establishing communication between nodes in mobile ad hoc networks (MANETs). In general, MANETs are autonomous mobile nodes, which can communicate over wireless links without any preinstalled infrastructure and it is useful on rescue operations. The main challenges in MANETs are frequent topology change; rely on battery power and absence of base stations. Thus the design of routing protocol should consider the adaptability, security, reachability and its energy efficiency. This paper discusses the QUAD based secured multipath routing protocol and its performance. In the protocol, messages are broadcasted only to limited nodes using QUAD scheme which can efficiently reduce the time to establish the path between source and destination nodes. Simulations are conducted to determine the performance characteristics of the protocol. The simulation results have shown excellent reduction of broadcast redundancy with QUAD and it maintains the level of existing security.

Key words: Protocol, mobile ad hoc network, security, multipath routing, LAR

INTRODUCTION

Mobile Ad hoc Networks (MANETs) consist of a set of wireless mobile nodes which communicate with one another without relying on any pre-existing infrastructure in the network. The distributed, wireless and self-configuring nature of MANETs make them suitable for a wide variety of applications (Toh, 2002). These include critical military operations, rescue and law enforcement missions as well as and disaster recovery scenarios (Stojmenovic, 2002). Other potential applications of MANETs are in data acquisition in hostile territories, virtual classrooms and temporary local area networks. Maintaining the availability of routes in MANETs during network runtime represents a challenging problem. In fact, they may be easily broken due to nodes mobility, links, node failure and radio interference. In addition, links could have limited bandwidth and network congestions would lead to resource starvation in nodes. Multipath routing algorithms were proposed to alleviate nodes these problems (Li and Wu, 2005) making a node able to establish and use simultaneously k paths to the destination (Shpungin and Segal, 2005).

A recent proposal by Bayrem (Triki *et al*., 2012) exhibits a secure multipath routing algorithm, which allows nodes in mobile ad hoc and sensor networks to perform an on-demand discovery and generation of a set of paths. He proposed an algorithm Secure Multipath Routing Algorithm for Mobile Adhoc and Sensor Networks (SeMuRAMAS) which is adaptive, secure and uses labels to carry the disjointness-threshold between nodes during the route discovery. It also uses security mechanisms based on the use of Watchdog and digital signature to protect the route discovery process.

Several multipath routing algorithms were proposed in the literature and each one trying to address certain problems with an existing algorithms or methods. Similarly, this paper is trying to address the route discovery problem exists with SeMuRAMAS. SeMuRAMAS is satisfied by the fact that source node is able to reconstruct all existing and shortest paths to the destination. But it broadcasts the RREQ over all nodes in the network including the Destination node.

Two particular topologies could reduce the considerably the performance of SeMuRAMAS. The first is obtained when nodes are so close to each other and all of them are located around the destination. In this topology, a RREQ generated from any node will reach all nodes in the network. As a result, a node could receive the same copy of datagrams from all nodes in the network. The nodes memory will be overloaded due to the highest number of paths to store in the Routing Path (RP) list which contains a copy of the RREQ previously discarded. The second is obtained when nodes are not deployed with sufficient number and most of nodes do not have more than two neighbours. The routing paths to generate will contain a large set of intermediate nodes. While the memory occupation rate in nodes is highly reduced with regard the previous topology, a multi-path will require a high delay to be established.

Corresponding Author: J. Viji Gripsy, Department of Computer Science, Psgrkc, Coimbatore, India

The general broadcasting principle followed by SeMuRAMAS is same as DSR. Broadcasting in MANETs is a fundamental data dissemination mechanism with number of important applications in route discovery and address resolution. Hence the change in broadcasting scheme may give better solution for time and energy required to establish the path between source and destination. Quad multipath routing protocol enhances the existing protocol (SeMuRAMAS). The Quad scheme is applied to reduce the network overhead.

The rest of paper organized as follows; the subsequent Section 2 reviews the related literatures, Section 3 describes the requirements of LAR, Section 4 presents the architecture of QUAD routing protocol, Section 5 describes about the results and discussion and the last part Section 6 depicts conclusion and future works.

RELATED WORKS

Network-wide broadcast is an essential feature for ad hoc networks. The simplest method for broadcast service is flooding. Its advantages are its simplicity and reachability. However, for a single broadcast, flooding generates abundant retransmissions resulting in battery power and bandwidth waste. Also, the retransmissions of close nodes are likely to happen at the same time. As a result, flooding quickly leads to message collisions and channel contention. This is known as the broadcast storm problem (Ni *et al*., 1999).

The broadcast problem has been extensively studied for multi-hop networks. Optimal solutions to compute Minimum Connected Domination Set (MCDS) (Guha and Khuller, 1996) were obtained for the case when each node knows the topology of the entire network (centralized broadcast). In particular, several solutions have been presented in which the broadcast time complexity is investigated in detail.

The broadcast protocol introduced in (Alon *et al*., 1991) completes the broadcast of a message in O (Dlog2n) steps where D is the diameter of the network and n is the number of nodes in the network. From the result proved in (Imielinski and Navas, 1996) this protocol is optimal for networks with constant diameter. For networks with a larger diameter, a protocol by (Gaber and Mansour, 1995; Guha and Khuller, 1996) completes the broadcast within O(D+log5n) time slots and it is optimal for networks with $D \in \Omega$ (log5n). These solutions are deterministic and guarantee a bounded delay on message delivery, but the requirement that each node must know the entire network topology is a strong condition, impractical to maintain in ad hoc mobile environments. Several broadcast protocols that do not require the knowledge of the entire network topology have been proposed. In a counter-based scheme (Ni *et al*., 1999) a node does not retransmit if it overhears the same message from its neighbours for more than a prefixed number of times and in a distance-based scheme (Ni *et al*., 1999), a node discards its retransmission if it overhears a neighbour within a distance threshold retransmitting the same message. Source Based Algorithm (Peng and Lu, 2000a) Dominant Pruning (Lim and Kim, 2000), Multipoint Relaying (Qayyum *et al*., 2000) Ad Hoc Broadcast Protocol (Peng and Lu, 2000b), DMPR (Vijendran and Gripsy, 2013). Lightweight and Efficient Network-Wide Broadcast Protocol (Sucec and Marsic, 2000) utilize 2-hop neighbour knowledge to reduce number of transmissions.

A good classification and comparison of most of the proposed protocols is presented in (Williams and Camp, 2002). It is also concluded that Scalable Broadcast Algorithm (SBA) (Peng and Lu, 2000a) and Ad Hoc Broadcast Protocol (AHBP) (Peng and Lu, 2000b) perform very well as the number of nodes in the network is increased. Both these techniques are based on two-hop neighbour knowledge.

In a survey of potential applications of GPS, (Dommety and Jain, 1996) briefly suggest use of location information in ad hoc networks, though they do not elaborate on how the information may be used. Other researchers have also suggested that location information should be used to improve (qualitatively or quantitatively) performance of a mobile computing system (Weiser, 1991; Spreitzer and Theimer, 1993). Metricom's Ricochet is a packet radio system using location information for the routing purpose (Metricom Web Page). The Metricom network infrastructure consists of fixed base stations whose precise location is determined using a GPS receiver at the time of installation.

Metricom uses a geographically based routing scheme to deliver packets between base stations. Thus, a packet is forwarded one hop closer to its final destination by comparing the location of packet's destination with the location of the node currently holding the packet. A routing and addressing method to integrate the concept of physical location (geographic coordinates), into the current design of the Internet, has been investigated in (Imielinski and Navas, 1996). DREAM is another protocol which maintains location information of each node in routing tables and sends data messages in a direction computed based on these routing (location) tables (Basagni *et al*., 1998). To maintain the location table accurately, each node periodically broadcasts a control packet containing its own coordinates, with the frequency of dissemination computed as a function of the node's mobility and

thedistance separating two nodes (called the distance effect). Unlike (Basagni *et al*., 1998) Location Aided Routing (LAR) (Ko and Vaidya, 2000) protocol using location information for route discovery, not for data delivery. Therefore the collective knowledge of reviews referred in this study suggest that making changes in broadcasting scheme primarily helps to reduce the traffic thereby it reduces the network overheads.

REQUIREMENTS OF LAR

The SeMuRAMAS extends the Dynamic Source Routing (DSR) algorithm, which is a reactive routing approach widely used as a basis for a large set of extended routing protocols. The phases in SeMuRAMAS are route discovery and route maintenance. The primary investigation of our proposal has two phases. First, apply the LAR broadcasting scheme associated with SeMuRAMAS and second, investigate the effectiveness of our proposed scheme with LAR+SeMuRAMAS.

This section describes the requirements of LAR for existing multipath routing algorithm. SeMuRAMAS capitalize the efficiency in terms of k-x connectivity, but with reference to the total network space the efficiency ratio is very less in our perspective. Therefore routing overhead is unavoidable and the RREQ will send to entire nodes in the network space. In order to improve the existing performance, we strongly believe the change in broadcasting scheme. In this study, we have presented Location Aided Routing (LAR) conjunction with SeMuRAMAS to make use of location information to reduce the routing overhead and maintain the security at k-x connectivity in multipath environment. Location information used in the LAR protocol may be provided by Global Positioning System (GPS) (Dommety and Jain, 1996). With the availability of GPS, it is possible for a mobile host to know its physical location. In reality, position information provided by the GPS includes some amount of error; in our scenario it is assumed as no error.

LAR contains two zones known as expected zone and request zone. The Expected zone is measured as follows: Consider a node S that needs to find a route to node D. Assume that node S knows that node D was at location L at time t_0 and that the current time is t_1 Then, the "expected zone" of node D, from the viewpoint of node S at time t_1, is the region that node S expects to contain node D at time t_1. Node S can determine the expected zone based on the knowledge that node D was at location L at time t_0. For instance, if node S knows that node D travels with average speed v, then S may assume that the expected zone is the circular region of radius v (t_1-t_0), centered at location L. If actual speed happens to be larger than the average, then the destination may actually be outside the expected zone at time t_1. Thus, expected zone is only an estimate made by node S to determine a region that potentially contains D at time t_1. In general, it is also possible to define v to be the maximum speed (instead of the average) or some other measure of the speed distribution. If node S does not know a previous location of node D, then node S cannot reasonably determine the expected zone-in this case, the entire region that may potentially be occupied by the ad hoc network is assumed to be the expected zone. In this case, LAR algorithm reduces the basic flooding algorithm. In general, having more information regarding mobility of a destination node can result in a smaller expected zone.

The Request zone is considered as follows: Consider a node S that needs to determine a route to node D. The proposed LAR algorithms use flooding with one modification. Node S defines (implicitly or explicitly) a request zone for the route request. A node forwards a route request only if it belongs to the request zone. To increase the probability that the route request will reach node D, the request zone should include the expected zone (described above). Additionally, the request zone may also include other regions around the request zone. There are two reasons: (a) When the expected zone does not include host S, a path from host S to host D must include hosts outside the expected zone. Therefore, additional region must be included in the request zone, so that S and D both belong to the request zone. (b) The request zone includes the expected zone, which means all paths from S to D include hosts that are outside the request zone. Thus, there is no guarantee that a path can be found consisting only have the hosts in a chosen request zone. Therefore, if a route is not discovered within a suitable timeout period, LAR protocol allows S to initiate a new route discovery with an expanded request zone. In our simulations, the expanded zone includes the entire network space. In this event, however, the latency in determining the route to D will be longer.

Note that the probability of finding a path (in the first attempt) can be increased by increasing the size of the initial request zone. However, route discovery overhead also increases with the size of the request zone. Thus, there exists a trade-off between latency of route determination and the message overhead. To address the route discovery overhead problem, we have proposed QUAD scheme to limit the network space according to the source and destination nodes. The subsequent section describes in detail about the QUAD scheme.

DESCRIPTION OF QUAD ROUTING

The proposed routing algorithm enforces the route discovery process in conjunction with LAR and SeMuRAMAS. Six kinds of datagram are used by QUAD during the route discovery:

- **Route request datagram:** Is the first packet to be broadcasted by a mobile node which wants to establish a multipath route to the destination mobile node. Every intermediate node exploits this datagram to discover incomplete routes in the network. It also appends it's identify in the RREQ and broadcasts it to its neighbours
- **Route response datagram:** Is sent back by the destination mobile node upon reception of the RREQ. This datagram contains the optimal path and is source routed to the node which generated the RREQ
- **Notification datagram:** Is used by the destination node to ask intermediate nodes to forward the information they learned regarding the routes to the source node. The information would have been invisible by the destination mobile node when it received the RREQ datagram
- **List forwarding datagram:** It is used by intermediate nodes to forward the information they stored regarding the existing paths in the network
- **Route error datagram:** It is sent by an intermediate node to the source node when it detects a route failure. It also lets the source node update the set of paths it uses to reach the destination mobile node
- **Threshold tuning datagram:** It is used by an intermediate node to indicate the value by which the threshold should be increased to let the establishment of the requested multiple paths be possible

Network discovery: When a mobile node, say S1 joins the network, it broadcasts a two-hop HELLO message, which includes its identity and has a Time To Live (TTL) value equal to 2 along with location information (X_i , Y_i) and timestamp t. Any node, say S2 which hears the message, includes the identity of S1 in its list of one-hop neighbours. This sets the TTL value of the HELLO message equal to 1 lower than its received value and forwards the datagram. Any node, say S3 that hears the message includes the identity of S2 in its list of one-hop neighbours and S1 in its list of two-hop neighbours and its sets the TTL value of the HELLO message equal to 1 lower than its received value and discards the datagram. To be considered as active, every node should periodically send a two-hop HELLO message and follow the above described process. This allows each node to maintain two up-to-date lists. The first is the list of neighbours and the second shows for each neighbour the list of its neighbours. The two lists will support the detection of routing attacks.

Route request generation and forwarding: A node which wants to establish a path to the destination mobile node say DN, initiates the route discovery by generating a RREQ datagram to DN and broadcasting it in the network. Prior to initiate the route discovery process, the following steps are involved: first step extracts the network space where the SN and DN belongs. In this case, we assume the network space as circular pattern and hence using circular sector formula the network space is divided into four regions:

$$A = \pi r^2 \bullet \frac{\theta^\circ}{360}$$

The region labels are nominated for each region in anticlockwise direction as Q1, Q2, Q3 and Q4. Now it initiates the second step, which tries to identify the regions where the SN, DN nodes are belonging. In this case minimum one region and maximum Q_n-1 regions may be selected for limiting the total network space. Hence at this point, the proposed broadcasting scheme will save atleast of 25% network space and eliminates the nodes belonging to the region. The third step triggered to limit the network region and the fourth step broadcast the RREQ to all nodes belongs to the selected regions and Fig. 1 illustrates the region.

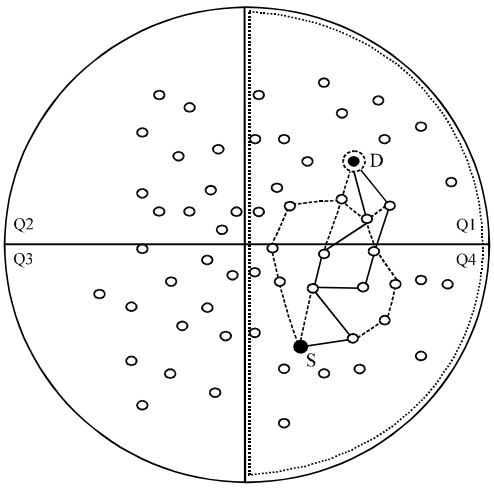

Fig. 1: QUAD broadcasting scheme

Every generated RREQ includes five-tuple information: <Seq, RREC, Dt, Loc, Region>. Seq stands for a sequence number which should be different for every new generated RREQ. The sequence number together with the IP address of the sender allows to uniquely identifying the RREQ and associates it to the subsequent generated responses. Dt is the disjointness threshold which is set by the sender to specify the maximal number of nodes that could be shared by any two paths among the set of paths to establish with the destination node. The value of Dt remains unchanged during the forwarding of the RREQ to the destination. RREC is a route record which is used to include the path followed by the RREQ to reach DN. In fact, when a node in the network receives a copy of this datagram for the first time, it appends its identity to the RREC field and broadcasted it to its neighbors. Every node, say N, including DN, which receives a second copy of the datagram, extracts the content of the RREC field. The latter provides a path from the sender to the node N. The node N will append the content of RREC together with the value of Seq to a list stored locally, entitled RP which stands for list of Received Paths. Then it discards the datagram. Loc contains the location information X_i, Y_i, t_i and Region refers the limited region to be broadcasted the RREQ.

Route response generation and forwarding: Once different copies of the RREQ datagram reach the destination node, later it will generate a Route Response datagram, say RREP, to the source. It includes four-tuple information <Seq, R, RCN, RPBS> where Seq represents the value of the sequence number that appeared within the received RREQ, R is the route, which is composed of the sequence of nodes which identifies the representing shortest path (between the source and the destination mobile node DN) among those that were received within the different copies of the RREQs. RCN stands for the remaining number of common nodes. It is initiated by DN to the value of x received within the RREQ. This value is decreased by 1 every time the RREP is routed by a node which contains a non empty list of received paths for the same value of the sequence number. The RREP datagram will be source routed to the sender based on the content of R. Moreover a list, say RPBS, containing the list of all the routing paths connecting the source node to DN is added to the RREP. When the RREP packet is routed to the source, the latter and all intermediate nodes will discover a route to DN, store it in their cache and use it as an alternative path if some link error will potentially occur. We remind the reader that any different routes requests, to be received by DN may share some nodes. Every route can be written as a series of nodes shared with other routes, followed by a series of distinct nodes.

Notification datagrams generation and forwarding: In this case where the destination mobile node MD has discarded a copy of the RREQ, it generates a notification datagram, say ND, containing the four-tuple information <Seq, RCN, L, RPBS> composed of the sequence number (Seq) and the value of RCN received in the RREP, in addition to a list L containing the identities of neighbour nodes from which a received copy of the RREQ was previously discarded (i.e., the identities of these neighbours stand for the last nodes in the routing paths provided by RP and related to the sequence number Seq). In this case where the ND is sent by the BS, the list L will be set to the identities of neighbour nodes from which a copy of the RREQ was received. RPBS is a list containing the set of routing paths connecting the source node to DN, including the shortest path. These routes are collected from the copies of the RREQ received by DN. The notification datagram ND is sent to the source node are broadcasted but treated only by the nodes existing in the list L.

In this case, where some node X in the network receives the RREP, two situations may happen. If X has already discarded atleast one copy of the related RREQ, it forwards it after decreasing the value of RCN and generates an ND containing the four-tuple information <Seq, RCN-1, L, RPBS>. If it is not the case, it simply forwards the datagram to its neighbours. When the intermediate node X receives a Notification datagram ND for the first time, two situations may happen. If X has not previously discarded any copy of the related RREQ, it simply forwards the NP to its neighbours.

If X has already discarded at least one copy of the related RREQ, it forwards it after decreasing the value of RNC and replacing the value of L by the identities of neighbour nodes from which a received copy of the RREQ was previously discarded. When X receives a second copy of the ND, it simply discards it. If the value RNC becomes equal to 0 after decreasing it by one, the notification packet will be rejected before sending it.

List forwarding datagrams generation and forwarding: Every node, which decreases the RCN's value of the Notification Datagram ND, generates a list forwarding datagram containing the sequence number (already received in the ND) and a list obtained from RP (the sequence number associated to RP should be the same as

the one received in the ND) after applying two filters, say F1 and F2, consecutively. The list forwarding datagram is sent to the source node (i.e., the node which initiated the RREQ). The first filter F1 eliminates from RP any path that has more than RCN-1 shared nodes with any path existing in RPBS. The second filter F2 locates in the output of F1 groups of nodes that share more than RCN-1 nodes. It replaces each one of these groups in the RP list by the shortest path. When the source node specifies a disjointness threshold x equal to 0 (i.e., all the discovered paths must be disjoint), the ND will be sent with a value of RCN equal to 0. Intermediate nodes receiving this latter and having an empty RP, should forward the packet to their neighbours. If it is not the case, they drop the notification datagram ND. Each time a node sends its RP list to the source node, it eliminates this list from its memory to preserve storage resources. If there is no additional space in the node memory, a solution consists in using the neighbour memory. Two categories of nodes can be used: nodes with high storage capacity and nodes with limited storage capacity. Each node knows the category of its neighbours. A node with a low storage capacity has the possibility to send parts of the data it stores only to neighbour nodes with high storage capacity. In fact, the receiving node should send back the data to the sender before it goes out of its coverage or sleeps. If the sender memory is still full, the receiving node should find a neighbour node, which is also a neighbour of the sender and has a high storage capacity, transfer the data to that node and inform the sender about its identity.

Threshold tuning datagram generation and forwarding: Each time that a mobile node sets the RCN to 0, it executes filters F1 and F2 along with the content of the RP to discard paths exceeding in terms of shared nodes in the authorized disjointness threshold. The mobile node computes the minimal number of shared nodes says n, between the remaining paths in the RP and sends this value to the source node within the TTD datagram. This value could be exploited by the source node, in the case where it is unable to establish the set of paths satisfying the requested threshold. In let it determines the best suitable threshold value that could be guaranteed by the network topology. This value will equal be n greater than the last used threshold value.

The subsequent section discuss about the limiting network space using QUAD scheme.

QUAD LNS Algorithm

```
// Limiting Network Space through QUAD broadcasting scheme
QUAD_LNS (Network Space, SN, DN)
{Find center point of the network space and radius;
        Classify the network space into quad format Q1,Q2,Q3,Q4;
        Evaluate the region of source and destination nodes;
        If (SN_Region == DN_Region)
        {// Limiting the network region
        Lm_Region = SN_Region;
        Return the Lm_Region;}
// if SN_Region is adjacent to DN_Region either way
Else if (SN_edge == DN_edge)
{// Merging of selected regions
        Lm_Region = SN_Region + DN Region;
        Return the Lm_Region;}
Else
{Predict the distance of DN from two adjacent
        quads of SN;
        // Intermediate Region
        Im_Region = Region has Less distance to DN;
        // Merging of selected regions
        Lm_Region = SN_Region + DN_Region + Im_Region;}}
```

The above algorithm states the unique steps involved in QUAD routing algorithm. The structure of SeMuRAMAS and LAR are briefly discussed by their respective authors. The role of LAR in QUAD embeds the location information and timestamp of each node to its neighbours. Thereby source node can find out the location of destination node with respect to the route cache. LAR with directional antenna can reduce the routing overhead and offers effectiveness. In this study we have considered only the general scenario which has found less impact on conventional method. In this connection, QUAD plays an important role in reducing the broadcast region and quickens the process of path establishment.

The above algorithm states that network range can be observed from the density of nodes in the network. Therefore, it is required to find out the center point and radius of the network space. The next step involves in slicing the network space based on the availability of information into quadruple format and assigns the region label. Algorithm now triggered to evaluate the belongingness of SN and DN node's region. If both SN_region and DN_region are same, it returns the Lm_region as SN_region; thus the original broadcasting range is limited to the specific range.

Otherwise, SN_region and DN_region are compared as adjacent region in either way. If both are adjacent, now the Lm_region trying to merge the SN_region and DN_region and return the Lm_region as limited network space. If the preceding conditions fail, it means that

SN_region and DN_region are belongs to opposite direction. Hence, this sequence is not advised to merge; because the center portion of the merging effect will be narrow band. In this scenario, the chances of communication between inter-region nodes are nearly impossible. Thus, intermediate region should be formed to avoid such kind of problems. In this case, we have two intermediate regions and the selection of appropriate region is measured in terms of distance function between neighbouring region and DN. Less distance indicates the closeness to the intermediate region. Therefore, SN_region, Im_region and DN_region are merged together as single limited network space. Subsequent section discuss about the simulation results and discussion.

RESULTS AND DISCUSSION

The proposed QUAD multipath routing algorithm and the existing SeMuRAMAS algorithms were tested in NS-2 simulation environment. Our simulation environment consists of mobile nodes in a rectangular region of size meters by meters. The nodes are randomly placed in the region and each of them has a radio propagation range of meters. The channel bandwidth is assumed to be Mb sec^{-1}. The Constant Bit Rate (CBR) flows are deployed for the data transmission. All nodes have the same transmission range of 250 m. The mobility model is the random waypoint model which is commonly used for simulating the movement pattern of mobile host in a MANET. For 50 nodes the simulation was carried out in a grid of 900×900 m, similarly for 100 and 150 nodes 1200 and 1500 m are applied. Table 1 depicts the basic parameters considered for this simulation.

Performance of SeMuRAMAS and QUAD is measured through three variables from the results, such as Packet Delivery Ratio (PDR) and memory overhead. PDR is a ratio of number of packets received to that of number of packets generated. If this rate is high then reliability of network is high. Similarly Routing load and route cost is also measured.

In this section, we present the results of our simulation. Every node periodically floods a message throughout the entire field. Low flooding rate has been chosen to minimize the packet loss due to buffer overflows and interference. All results generated from the simulation are based on the average runs of uniform node distributions and in general, the variance of results for ad hoc network seems high which is happened due to randomness of certain resources.

Table 1: Simulation setup

Parameters	Value
Transmission range (M)	250
Bandwidth (Mbps)	512
Max. node speed (m sec^{-1})	7
Pause time (sec)	0
Packet size (Kb)	1000
Average TTL (sec)	40
No. of data items	1000
Traffic	CBR
Simulation time (sec)	20
No. of nodes	50, 100, 50

Table 2: Results of SeMuRAMAS and QUAD

Parameters	Nodes		
No. of nodes	50	100	150
PDR-SeMuRAMAS	80.9	71.83	69.01
PDR-QUAD	94.5	96.06	96.06

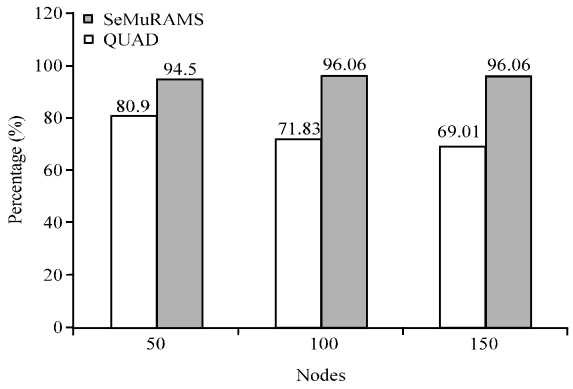

Fig. 2: PDR of SeMuRAMAS and QUAD

The effectiveness of existing and proposed method is measured using PDR, routing load and routing cost. Table 2 depicts the performance of SeMuRAMAS under 50, 100 and 150 nodes. The result states that 80.9% PDR is achieved at 50 nodes, but in 100 and 150 nodes the PDR is reduced to 71.83 and 69.01; whereas QUAD result depicts as 94.5, 96.06 and 96.06. Figure 2 confirmed the QUAD routing is better performing compared to SeMuRAMAS. The routing load in both cases persistently increasing when the number of nodes increases. But the ratio of increase is not identical in this scenario.

The above Fig. 3 depicts the memory overhead performance of SeMuRAMAS & QUAD. When the RREQ datagram is forwarded, every node which received a copy stores the route record in its list of received paths. Since this list is temporarily stored within the mobile node memory, we estimate the average number of stored paths in each node in terms of the number of nodes. The result exhibits QUAD performance seems identical to

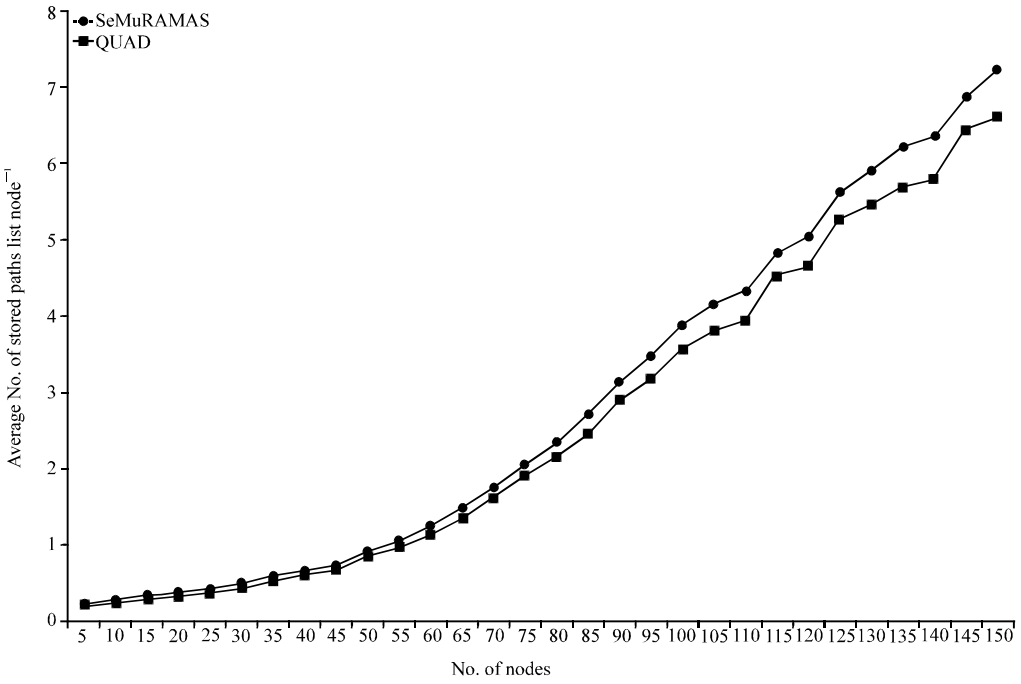

Fig. 3: Memory Overhead SeMuRAMAS and QUAD

SeMuRAMAS in many situations. But it acquires some amount of efficiency which states that 7.56% of efficiency on memory overhead handlings. The computation of memory overhead is observed from (Triki *et al*., 2012).

CONCLUSION

In this study, QUAD multipath routing protocol is evaluated, which enhance the existing proposal known as SeMuRAMAS. LAR is used to embed the location information in the routing packet. Further, the QUAD scheme is applied to reduce the network space by QUAD_LNS sequence between source and destination nodes. The performance evaluation between SeMuRAMAS and QUAD confirms the QUAD routing is performing better. The original effect on QUAD is not achieved due to existing procedures of SeMuRAMAS, hence future work should address on threshold value and reduce the overheads.

REFERENCES

Alon, N., A. Bar-Noy, N. Linial and D. Peleg, 1991. A lower bound for radio broadcast. J. Comput. Syst. Sci., 43: 290-298.

Basagni, S., I. Chlamtac, V.R. Syrotiuk and B.A. Woodward, 1998. A distance routing effect algorithm for mobility (DREAM). Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, October 25-30, 1998, Dallas, Texas, USA., pp: 76-84.

Dommety, G. and R. Jain, 1996. Potential networking applications of global positioning system (GPS). Technical Report TR-24, CS Department, The Ohio State University, USA.

Gaber, I. and Y. Mansour, 1995. Broadcast in radio networks. Proceedings of the 6th Annual ACM-SIAM Symposium on Discrete Algorithms, January 22-24, 1995, San Francisco, USA., pp: 577-585.

Guha, S. and S. Khuller, 1996. Approximation algorithms for connected dominating sets. Proceedings of the 4th Annual European Symposium on Algorithms, September 25-27, 1996, Barcelona, Spain, pp: 179-193.

Imielinski, T. and J.C. Navas, 1996. GPS-Based addressing and routing. Technical Report LCSR-TR-262, Rutgers University, USA.

Ko, Y.B. and N.H. Vaidya, 2000. Location-Aided Routing (LAR) in mobile ad hoc networks. Wireless Networks, 6: 307 -321.

Li, S. and Z. Wu, 2005. Node-Disjoint parallel multi-path routing in wireless sensor networks. Proceedings of the 2nd International Conference on Embedded Software and Systems, December 16-18, 2005, China, pp: 432-443.

Lim, H. and C. Kim, 2000. Multicast tree construction and flooding in wireless ad hoc networks. Proceedings of the ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, August 20, 2000, Boston, UK., pp: 61-68.

Ni, S.Y., Y.T. Chen and J.P. Sheu, 1999. The broadcast storm problem in a mobile ad hoc network. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 15-19, 1999, Seattle, WA., USA., pp: 151-162.

Peng, W. and X. Lu, 2000a. AHBP: An efficient broadcast protocol for mobile ad hoc networks. J. Sci. Technol. (Beijing, China), 6: 32-40.

Peng, W. and X. Lu, 2000b. On the reduction of broadcast redundancy in mobile ad hoc networks. Proceedings of 1st ACM International Symposium on Mobile ad hoc Networking and Computing, August 11, 2000, Boston, MA., USA., pp: 129-130.

Qayyum, A., L. Viennot and A. Laouiti, 2000. Multipoint relaying: An efficient technique for flooding in mobile wireless networks. Technical Report 3898, INRIA-Rapport.

Shpungin, H. and M. Segal, 2005. K-Fault resistance in wireless ad-hoc networks. Proceedings of the Joint Workshop on Foundations of Mobile Computing, September 2, 2005, Germany, pp: 89-96.

Spreitzer, M. and M. Theimer, 1993. Providing location information in a ubiquitous computing environment. Proceedings of the 14th ACM Symposium on Operating Systems Principles, December 5-8, 1993, USA., pp: 270-283.

Stojmenovic, I., 2002. Handbook of Wireless Networks and Mobile Computing. Wiley, New York, USA.

Sucec, J. and I. Marsic, 2000. An efficient distributed network-wide broadcast algorithm for mobile ad hoc networks. CAIP Technical Report 248, September, 2000, Rutgers University, USA.

Toh, C.K., 2002. Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall, Upper Saddle River, New Jersey, USA.

Triki, B., S. Rekhis and N. Boudriga, 2012. Threshold based multipath routing algorithm in mobile ad hoc and sensor networks. Proceedings of the 7th International Joint Conference on E-Business and Telecommunications, July 26-28, 2010, Athens, Greece, pp: 54-70.

Vijendran, A.S. and J.V. Gripsy, 2013. Scalable and secured route discovery mechanism using DSR protocol. Eur. J. Sci. Res., 101: 177-184.

Weiser, M., 1991. The computer for the 21st century. Sci. Am., 265: 94-104.

Williams, B.T. and T. Camp, 2002. Comparison of broadcasting techniques for mobile ad hoc networks. Proceedings of the 3rd International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, New York, USA., pp: 194-205.